

Quantum Secure Direct Communication between Two Strangers

Tzonelih Hwang*, Tzu-Han Lin, and Shih-Hung Kao

February 28, 2014

Abstract

This paper presents the first quantum secure direct communication (QSDC) protocol for two strangers, who do not pre-share any secret and even not having any authentication channel between them. The proposed protocol only requires the help of two dishonest third parties (TPs) to achieve the goal. The security analyses show that the proposed protocol is secure against not only the external eavesdropper's attack, but also the dishonest TP's attack.

PACS: 03.67.Dd, 03.67.Hk

Keywords: Quantum Cryptography, Dishonest Third Party, Quantum Communication

1 Introduction

Consider the following scenario: Alice, a project manager who works at a head office of a company, is asked to merge her project with Bob, a project manager

*Corresponding author

hwangtl@ismail.csie.ncku.edu.tw

Department of Computer Science and Information Engineering, National Cheng Kung University, No. 1, University Rd., Tainan City, 701, Taiwan, R.O.C.

works at the branch office of the same company. Though they are working for the same company, they never met before. To merge the project, they have to do lots of private communications because the project they are handling is confidential. Alice insists that no one, except Bob, is able to reveal the content of their communication. What should they do?

Conventionally, they have to establish a secret channel between them. With the symmetric-key cryptography, Alice and Bob have to first pre-share a key of a cryptosystem, e.g., AES. Then Alice, the sender, can encrypt her message using the shared key, and transmit the ciphertext to Bob via public classical channel. However, since Alice and Bob did not meet each other before, they cannot exchange the secret key even face-to-face. To share a secret key, they have to look for a third party (TP,) who respectively shares keys with them, and ask TP to distribute a session key for them [1–3]. Then, Alice and Bob can encrypt/decrypt the private information, and thus a secure communication is possible.

Since the shared secret key between Alice and Bob is distributed by the TP. TP has to be honest enough, not spying on Alice and Bob’s communication, otherwise, Alice and Bob’s secret might be revealed by TP.

Though the development of quantum cryptography in recent years, e.g., the BB84 quantum key distribution (QKD) [4], allows two users to distribute a secret key without pre-sharing a key, it requires that an authenticated classical channel is pre-established between the two communicants. For two users who do not know each other, they cannot establish any authentication channel between them directly, and hence a TP should be there to serve as a bridge of an authenticated classical channel between both strangers [5–7]. The use of quantum mechanics in cryptography allows this TP to be a semi-honest agent who will loyally execute the protocol, but may try to reveal Alice and Bob’s secret with

the public information, a scenario not possible in the conventional cryptography, where TP can easily eavesdrop Alice and Bob's communication without being detected, and hence as we mention earlier the TP in the conventional cryptography has to be complete honest and trusted.

However, if the TP in the quantum cryptographic protocols is dishonest, in the sense that he/she may deviate from the normal procedure of the protocol in order to reveal Alice's secret. That is, the TP not only can passively collect useful information, but also can actively perform any attack on the protocol except conspiring with the participant. In this case, Alice and Bob, who do not directly share an authenticated channel, may not be able to detect and avoid the TP's attack, and their secret information might be thus leaked to the TP [8]. Under this scenario, can we develop a secure protocol for a pair of strangers to exchange private information under the help of dishonest TPs?

This paper aims to answer this question by proposing a new strategy, which allows Alice and Bob, who do not know each other before, to establish a secure communication via the help of untrusted TPs. To achieve this goal, Alice and Bob can simply look for one TP respectively to join the protocol. In the proposed environment, Alice and Bob can directly communicate privately, and each of the two TPs can respectively help Alice and Bob to detect the other TP's illegal behavior.

The rest of this paper is organized as follows: Section 2 introduces the proposed environment. Section 3 describes the proposed quantum secure direct communication (QSDC) protocol between two strangers. Section 4 gives the security analyses of the proposed protocol. Finally, the conclusions will be given in Section 5.

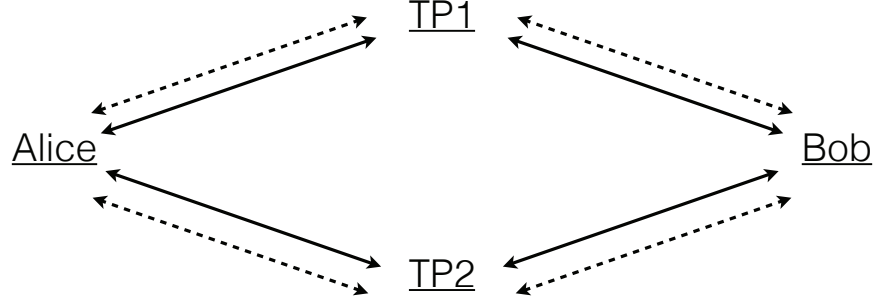


Figure 1: The Proposed Environment

2 The Environment

In this section, the proposed environment and its security requirement are described. The environment, including two communicants, Alice and Bob, and two TPs, TP1 and TP2, is described as follows. (see also Fig. 1, where the dotted lines denote the quantum channels, and the solid lines denote the authenticated classical channels.)

1. Alice (Bob) shares authenticated classical channels and quantum channels with two TPs, respectively.
2. The transmitted information on the authenticated classical channel is public, but the receiver can verify its integrity and originality.
3. TPs are dishonest in the sense that they can perform any possible attacks except conspiring with Alice, or Bob, or the other TP.
4. An external attacker, Eve, may try to perform any attack to disturb, forge, or eavesdrop Alice and Bob's communication.

3 Quantum Secure Direct Communication Protocol for the Proposed Environment

This section presents a quantum secure direct communication (QSDC) protocol for the proposed environment. The proposed QSDC protocol allows the sender, Alice to send a secret message to a stranger Bob without pre-sharing any secret with him. In the proposed QSDC protocol, though the quantum signals are generated by TP1, Alice and Bob can determine if TP1 performs any attack on the quantum signals via the help of TP2. The QSDC protocol proceeds as follows:

(Step1) TP1 generates a sequence of EPR entangled states, $|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{12}$,

where the subscripts 1 and 2 denote respectively the first and the second qubits. Let Q_1 (Q_2) denotes the particle sequence includes all the first (second) qubit of each EPR state in order. TP1 then inserts enough amount of decoy photons [9–11] randomly chosen from the four states: $\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ into Q_1 (Q_2) to form a new sequence S_1 (S_2 .) TP1 sends the sequence S_1 to Alice, and S_2 to Bob, respectively.

(Step2) Once Alice receives the quantum sequence S_1 from TP1, she sends an acknowledgement to TP1 via the authenticated classical channel. TP1 and Alice then will publicly discuss the decoy photons for the eavesdropping detection. TP1 informs the position and the basis of each decoy photon to Alice. Alice measures these decoy photons, and then sends the measurement results to TP1. By comparing the initial states and the measurement results, TP1 can detect the existence of eavesdroppers. Similarly, Bob will also publicly discuss the decoy photons in S_2 with TP1. In addition, Alice has to use the photon number splitter (PNS) and the wavelength filter to

check if Trojan Horse attacks exist in the protocol [12–15].

(Step3) If the quantum transmissions are free from the eavesdroppers and the Trojan Horse attacks, Alice and Bob can remove the decoy photons and recover the sequences Q_1 and Q_2 . They then will discuss the entanglement of the shared EPR states via the help of TP2. TP2 randomly selects the position and basis (X basis or Z basis) for each photon to be checked and announces the positions and bases to Alice and Bob. Alice and Bob then measure the selected particles in Q_1 (Q_2) with the bases chosen by TP2, and sends the measurement results to TP2. Because

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}} (|++\rangle + |--\rangle) \end{aligned} \quad (1)$$

, TP2 can compare the measurement results from Alice to Bob to determine if Alice and Bob's qubits are in $|\Phi^+\rangle$.

(Step4) If the entanglement correlations between Alice's and Bob's qubits are correct, Alice (Bob) will remove the measured qubits selected by TP2 from Q_1 (Q_2), and have a new sequence, Q'_1 (Q'_2). To transmit her secret message, Alice applies dense coding on her photons by performing unitary operation on each qubit of Q'_1 according to her two-bit messages. If the two-bit message is 00, she will perform $I = |0\rangle\langle 0| + |1\rangle\langle 1|$; if the two-bit message is 01, she will perform $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$; if the two-bit message is 10, she will perform $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$; otherwise, she will perform $i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$. After the encoding, Alice generates decoy photons as in Step 1 by TP1, and inserts them to Q'_1 to form a new sequence S'_1 , which is then transmitted to TP2. Upon receiving S'_1 , TP2 publicly discusses the decoy photons with Alice as in Step2. If there are eavesdroppers detected, they will abort the protocol and return to Step 1.

(Step5) TP2 removes the decoy photons from S'_1 , and inserts new decoy photons into the particle sequence to form S''_1 , which is then transmitted to Bob.

(Step6) Bob and TP2 again discuss the decoy photons for detecting the eavesdroppers. If the quantum transmission between TP2 and Bob is secure, Bob can remove the decoy photons and obtain the particle sequence Q'_1 . Bob then performs Bell measurement (EPR measurement) on every pair of qubits respectively from Q'_1 and Q'_2 . According to the measurement results, Bob can obtain Alice's secret message. (See Eq. (2))

$$\begin{aligned}
I |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = |\Phi^+\rangle \\
\sigma_z |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) = |\Phi^-\rangle \\
\sigma_x |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) = |\Psi^+\rangle \\
i\sigma_y |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) = |\Psi^-\rangle
\end{aligned} \tag{2}$$

4 Security Analyses

This section analyzes the security of the proposed QSDC protocol. First, the general attack, i.e., the entangled-and-measure attack is considered, then, some well-known attacks are analyzed.

The Entangle-and-measure Attack

When TP1 sends S_1 to Alice in Step 1, the external eavesdropper, Eve, may perform the entangle-and-measure attack [16–18] to steal the information in the transmitted qubits in S_1 . Because S_1 contains TP1's decoy photons, to avoid being detected, Eve will try to obtain the state of the decoy photons. For each qubit, q_1 , in S_1 , Eve prepares an ancillary qubit in an arbitrary known state $q_e = |E\rangle$, and performs her attack operation U on q_1 and q_e . The result of Eve's

operation is as follows:

$$\begin{aligned}
U|0\rangle_1|E\rangle_e &= a|0\rangle_t|e_{00}\rangle_e + b|1\rangle_t|e_{01}\rangle_e \\
U|1\rangle_1|E\rangle_e &= c|0\rangle_t|e_{10}\rangle_e + d|1\rangle_t|e_{11}\rangle_e \\
U|+\rangle_1|E\rangle_e &= \frac{1}{2} \begin{bmatrix} |+\rangle_t(a|e_{00}\rangle_e + b|e_{01}\rangle_e + c|e_{10}\rangle_e + d|e_{11}\rangle_e) + \\ |-\rangle_t(a|e_{00}\rangle_e - b|e_{01}\rangle_e + c|e_{10}\rangle_e - d|e_{11}\rangle_e) \end{bmatrix} \\
U|-\rangle_1|E\rangle_e &= \frac{1}{2} \begin{bmatrix} |+\rangle_t(a|e_{00}\rangle_e + b|e_{01}\rangle_e - c|e_{10}\rangle_e - d|e_{11}\rangle_e) + \\ |-\rangle_t(a|e_{00}\rangle_e - b|e_{01}\rangle_e - c|e_{10}\rangle_e + d|e_{11}\rangle_e) \end{bmatrix}
\end{aligned} \tag{3}$$

, where $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$, and $|e_{11}\rangle$ are four states which Eve can distinguish, and $|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1$.

To pass the eavesdropping detection, Eve sets $b = c = 0$ and $(a|e_{00}\rangle_e + b|e_{01}\rangle_e + c|e_{10}\rangle_e + d|e_{11}\rangle_e) = (a|e_{00}\rangle_e + b|e_{01}\rangle_e - c|e_{10}\rangle_e - d|e_{11}\rangle_e) = \vec{0}$. Eve's operation thus will not change the state of q_1 , and Eve can successfully pass the eavesdropping detection. However, $b = c = 0$ implies $(a|e_{00}\rangle_e - d|e_{11}\rangle_e) = \vec{0}$, that is, $a|e_{00}\rangle_e = d|e_{11}\rangle_e$. In this case, Eve cannot distinguish $|e_{00}\rangle$ and $|e_{11}\rangle$, and she cannot obtain the information in q_1 . If Eve wants to distinguish $a|e_{00}\rangle_e$ from $d|e_{11}\rangle_e$, her operation, U , will change the state of q_1 , which will cause her attack to be detected by TP1 and Alice.

Generally, if Eve want to pass the eavesdropping check, she cannot get any information. If Eve tries to reveal the whole information from a qubit, she will change the state of the qubit, and eventually be detected in the public discussion.

Special Attacks

The above analysis shows that the proposed QSDC protocol is secure against the entangled-and-measure attack. However, it has been shown that some special

attacks can be successful even if the protocol is proven to be secure against the entangled-and-measure attack [8, 12–15, 19–23]. Hence, the following security analyses will focus on some special attacks: the correlation-elicitation attack, the dense coding attack, and the entanglement swapping attack.

The Correlation-elicitation Attack

The dishonest TP2 may try to steal Alice's secret by performing the correlation-elicitation (CE) attack [19–22]. When the second qubit of the EPR state generated by TP1 (denoted as q_2) is transmitted to Bob in Step 1, TP2 intercepts it, and generates an ancillary photon $q_e = |0\rangle$. TP2 then performs the first controlled-NOT (CNOT) operation on q_2 and q_e , where q_2 is the control bit, and q_e is the target bit. As a result, the two-particle EPR state and the ancillary photon can be described as follows:

$$CNOT_{2e} |\Phi^+\rangle_{12} \otimes |0\rangle_e = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) \quad (4)$$

, where \otimes denotes the tensor product operation. TP2 then resends q_2 to Bob. When Alice sends the encoded first qubit, q_1 , of the EPR state to TP2 in Step 5, TP2 performs the second CNOT operation on q_1 and q_e , where q_1 is the control bit, and q_e is the target bit. Due to Alice's encoding operation, the state of q_1 and q_2 becomes one of $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$ (see Eq. (2).) The four possible states after the second CNOT operation are as follows:

$$\begin{aligned} CNOT_{1e} CNOT_{2e} |\Phi^+\rangle_{12} \otimes |0\rangle_e &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{12} \otimes |0\rangle_e \\ CNOT_{1e} CNOT_{2e} |\Phi^-\rangle_{12} \otimes |0\rangle_e &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)_{12} \otimes |0\rangle_e \\ CNOT_{1e} CNOT_{2e} |\Psi^+\rangle_{12} \otimes |0\rangle_e &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)_{12} \otimes |1\rangle_e \\ CNOT_{1e} CNOT_{2e} |\Psi^-\rangle_{12} \otimes |0\rangle_e &= \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)_{12} \otimes |1\rangle_e \end{aligned} \quad (5)$$

TP2 is now able to obtain Alice's partial secret according to the Z-basis measurement result of q_e . According to Eq. (5,) if the measurement result of q_e is $|0\rangle$, TP2 knows that the state of q_1 and q_2 is either $|\Phi^+\rangle$ or $|\Phi^-\rangle$; otherwise, the state is $|\Psi^+\rangle$ or $|\Psi^-\rangle$. TP2 can thus obtain partial information about Alice's secret message. However, when TP1 sends the sequence S_2 , which includes q_2 of each EPR pair, to Bob, S_2 also contains TP1's decoy photons, where the positions and bases of these decoy photons are unknown to TP2. If TP2's first CNOT operation is performed on an X-basis decoy photon, for example, $q_d = |+\rangle$, the result is as follows:

$$CNOT_{de} |+\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}} (|++\rangle + |--\rangle)_{de} \quad (6)$$

It can be seen that if Bob measures the decoy photon in X basis, the measurement result will be $|+\rangle$ or $|-\rangle$ with an equal probability of 50%. Hence, if the decoy photon is in X basis, TP2's attack may disturb the state of decoy photon. Eventually, it causes TP2 to be detected with a probability of 50%. However, if the decoy photon is in Z basis, TP2's first CNOT operation will not disturb the state. Assume that TP1 selects the basis of each decoy photons with equal probability in Z basis or X basis, TP2's attack will be detected with the following probability: $50\% \times 50\% + 50\% \times 0 = 25\%$. Consequently, if there are n decoy photons, the detection rate of TP2's attack is $1 - (25\%)^n$. If n is large enough, the probability will be close to 1.

The Dense Coding Attack

The external attacker, Eve, may try to perform the dense coding attack [23] to reveal Alice's secret message. When TP1 transmits S_1 to Alice in Step 2, Eve intercepts it, and prepares a sequence of EPR states $|\Phi^+\rangle_{e1,e2}$, where $e1$ and $e2$ respectively denote the first and the second particles of the EPR states

generated by Eve. Eve sends all q_{e1} , the first particle of each EPR state, to Alice in hope that she successfully passes the eavesdropping detection, and thus Alice's encoding operations will be performed on Eve's q_{e1} . Consequently, when Alice sends out the encoded qubits to TP2 in Step 5, Eve can retrieve her q_{e1} and performs EPR measurement on every pair of q_{e1} and q_{e2} . That is, according to the measurement results (see Eq. (2),) Eve can reveal Alice's secret message. However, S_1 contains decoy photons. According to Eq. (1,) it can be seen that the first particle has two measurement results in both two basis. If the original decoy photon is $|1\rangle$, and Alice measures the fake photon, q_{e1} , in Z basis, then the measurement result will be $|0\rangle$ or $|1\rangle$ with equal probability. If the measurement result is $|0\rangle$, Eve's attack will be detected. For each decoy photon, Alice will get an illegal measurement result on Eve's fake photon with the probability of 50%. Let n be the number of decoy photons, Eve's attack will be detected with the probability of $1 - (50\%)^n$. If n is large enough, the probability will be close to 1.

The Entanglement Swapping Attack

TP1, who generates the EPR states for Alice and Bob, may also try to perform the entanglement swapping attack [8] to obtain Alice's secret message. In Step 1, instead of generating one EPR pair and distributing these two particles to Alice and Bob, respectively, TP1 generates two EPR pairs, namely $|\Phi^+\rangle_{T1,T2}$ and $|\Phi^+\rangle_{T3,T4}$. TP then distributes q_{T1} , the first particle of the first EPR state, to Alice, and q_{T3} , the first particle of the second EPR state, to Bob. Because all the decoy photons are generated by TP1, TP1 can successfully pass the eavesdropping check of decoy photons in Step 2. If the entanglement correlation check in Step 3 can be passed, in Step 5, Alice will send the encoded particle, q_{T1} to TP2. TP1 can intercept them, remove the decoy photons according to Alice and TP2's public communication, and perform an EPR measurement on

the qubit pair q_{T1} and q_{T2} . According to the measurement result, TP1 can obtain Alice's secret message.

But the fact is, when Alice, TP2, and Bob discuss the entanglement of the shared EPR states in Step 3, for each discussed position, TP1 can measure the qubit pair q_{T2} and q_{T4} . The qubits q_{T1} and q_{T3} then will be in one of four EPR states, $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, which is also known by TP1. Because these two particles held respectively by Alice and Bob are still in EPR state, they cannot detect that TP1 generated two EPRs rather than one. However, the above situation happens only when TP1 is allowed to generate variable EPR states. In the proposed protocol, however, TP1 is only allowed to generate $|\Phi^+\rangle$, if he/she performs above attack, the EPR state shared by Alice and Bob in public discussion will be in one of $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, rather than in $|\Phi^+\rangle$ as in normal situation. For example, if the shared state is $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, Alice's and Bob's Z-basis measurement will be $|0\rangle$ and $|1\rangle$ ($|1\rangle$ and $|0\rangle$), whereas the legal measurement results is $|0\rangle$ and $|0\rangle$ ($|1\rangle$ and $|1\rangle$). TP1's attack thus will be detected by TP2. The proposed protocol is thus secure against TP1's entanglement swapping attack.

The above analyses show that the proposed protocol is not only secure against the general attack, but also secure against some special attacks. If TP1 attacks the protocol, he/she will be detected in the public discussion held by TP2 in Step 3. Similarly, if TP2 attacks the protocol, he/she will be detected in Step 2, the public discussion of decoy photons generated TP1. Two dishonest TPs, TP1 and TP2, share duty to watch each other and as a result, two strangers, Alice and Bob can have a secure communication between each other.

5 Conclusions

This paper presents a new research in quantum cryptography, which allows two strangers to have a QSDC via the help of two dishonest TPs. Each TP is designed to prevent the other TP from acting maliciously, and hence, both TPs can be dishonest. Because the proposed QSDC enables both strangers to share EPR pairs, it can also be easily transformed to a quantum teleportation, quantum key distribution, quantum private comparison, and etc. between two strangers. It indeed is a challenge to resolve this scenario, secure communication between two strangers, using other approaches. And it would be even interesting to have a secure quantum communication anonymously between strangers.

Acknowledgment

This research is supported partially by the National Science Council, Taiwan, R.O.C., under the Contract No. NSC 100-2221-E-006-152-MY3.

References

- [1] R. K. Bauer, T. A. Berson, and R. J. Feiertag, “A key distribution protocol using event markers,” *ACM Trans. Comput. Syst.*, vol. 1, no. 3, pp. 249–255, Aug. 1983.
- [2] R. M. Needham and M. D. Schroeder, “Using encryption for authentication in large networks of computers,” *Commun. ACM*, vol. 21, no. 12, pp. 993–999, Dec. 1978.
- [3] R. M. Needham and M. D. Schroeder, “Authentication revisited,” vol. 21, no. 1. New York, NY, USA: ACM, 1987, pp. 7–7.

- [4] C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, vol. 175, 1984, pp. 175–179.
- [5] T. Hwang, K.-C. Lee, and C.-M. Li, “Provably secure three-party authenticated quantum key distribution protocols,” *IEEE Trans. Dependable Secur. Comput.*, vol. 4, no. 1, pp. 71–80, 2007.
- [6] H.-C. Shih, K.-C. Lee, and T. Hwang, “New efficient three-party quantum key distribution protocols,” *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 15, no. 6, pp. 1602–1606, 2009.
- [7] W. Q.-Y. Yang Yu-Guang, “Economical multiparty simultaneous quantum identity authentication based on greenberger–horne–zeilinger states,” *Chin. Phys. B*, vol. 18, no. 8, pp. 3233–3237, 2009.
- [8] W.-W. Zhang and K.-J. Zhang, “Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party,” *Quantum Information Processing*, pp. 1–10, 2012.
- [9] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.
- [10] C.-Y. Li and et al., “Secure quantum key distribution network with bell states and local unitary operations,” *Chinese Physics Letters*, vol. 22, no. 5, p. 1049, 2005.
- [11] C.-Y. Li, X.-H. Li, F.-G. Deng, P. Zhou, Y.-J. Liang, and H.-Y. Zhou, “Efficient quantum cryptography network without entanglement and quantum memory,” *Chinese Physics Letters*, vol. 23, no. 11, p. 2896, 2006.
- [12] F.-G. Deng, X.-H. Li, H.-Y. Zhou, and Z.-j. Zhang, “Improving the security

- of multiparty quantum secret sharing against trojan horse attack," *Physical Review A*, vol. 72, no. 4, p. 044302, 2005.
- [13] Q.-Y. Cai, "Eavesdropping on the two-way quantum communication protocols with invisible photons," *Physics Letters A*, vol. 351, no. 1-2, pp. 23–25, 2006.
- [14] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, "Improving the security of secure direct communication based on the secret transmitting order of particles," *Physical Review A*, vol. 74, no. 5, p. 054302, 2006.
- [15] S.-K. Chong, Y.-P. Luo, and T. Hwang, "On "arbitrated quantum signature of classical messages against collective amplitude damping noise",," *Optics Communications*, vol. 284, no. 3, pp. 893–895, 2011.
- [16] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block," *Physical Review A*, vol. 68, no. 4, p. 042317, 2003.
- [17] F. Gao, F. Guo, Q. Wen, and F. Zhu, "Comparing the efficiencies of different detect strategies in the ping-pong protocol," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 51, no. 12, pp. 1853–1860, 2008.
- [18] T.-Y. Wang, Q.-Y. Wen, and F.-C. Zhu, "Secure authentication of classical messages with single photons," *Chinese Physics B*, vol. 18, no. 8, p. 3189, 2009.
- [19] S.-J. Qin, Q.-Y. Wen, and F.-C. Zhu, "An external attack on the brádler–dušek protocol," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 40, no. 24, p. 4661, 2007.
- [20] F. Gao, S. Lin, Q.-Y. Wen, and F.-C. Zhu, "A special eavesdropping on one-

- sender versus n -receiver qsd protocol,” *Chinese Physics Letters*, vol. 25, no. 5, p. 1561, 2008.
- [21] S.-J. Qin, F. Gao, Q.-Y. Wen, L.-M. Meng, and F.-C. Zhu, “Cryptanalysis and improvement of a secure quantum sealed-bid auction,” *Optics Communications*, vol. 282, no. 19, pp. 4014–4016, 2009.
- [22] F. Gao, S.-J. Qin, Q.-Y. Wen, and F.-C. Zhu, “Cryptanalysis of multiparty controlled quantum secure direct communication using greenberger-horne-zeilinger state,” *Optics Communications*, vol. 283, no. 1, pp. 192–195, 2010.
- [23] G. Fei, Q. Su-Juan, G. Fen-Zhuo, and W. Qiao-Yan, “Dense-coding attack on three-party quantum key distribution protocols,” *Quantum Electronics, IEEE Journal of*, vol. 47, no. 5, pp. 630–635, 2011.